Software Engineering Institute

Defining a Maturity Scale for Governing Operational Resilience

Katie Stewart
Julia Allen
Audrey Dorofee
Michelle Valdez
Lisa Young

March 2015

TECHNICAL NOTE
CMU/SEI-2015-TN-004

CERT Division

http://www.sei.cmu.edu

Carnegie Mellon

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

Table of Contents

List of Figures

List of Tables

Acknowledgments

The authors would like to thank Matthew Butkovic and Rich Caralli for their thought leadership around Maturity Indicator Levels (MILs) and detailed review of this report. We would also like to thank Jim Cebula and Summer Fowler for their leadership and sponsorship of this ongoing research effort.

Abstract

Achieving operational resilience in today's environment is becoming increasingly complex as the pace of technology and innovation continues to accelerate. Sponsorship, strategic planning, and oversight of operational resilience are the most crucial activities in developing and implementing an effective operational resilience management (ORM) system. These governance activities are described in detail in the CERT® Resilience Management Model enterprise focus (EF) process area (PA). To ensure operational resilience, an organization must identify shortfalls across these defined activities, make incremental improvements, and measure improvement against a defined, accepted maturity scale. The current version of the CERT Resilience Management Model (CERT-RMM V1.2) utilizes a maturity architecture (levels and descriptions) that may not meet the granularity needs for organizations committed to making incremental improvements in governing operational resilience. To achieve a more granular approach, the CERT-RMM Maturity Indicator Level (MIL) scale was developed for application across all CERT-RMM PAs. The CERT Division of Carnegie Mellon University's Software Engineering Institute is conducting ongoing research around the current state of the practice of governing operational resilience and developing specific actionable steps for improving the governance of operational resilience. Study results provide the specific EF PA MIL scale for assessing maturity, identifying incremental improvements, and measuring improvements.

1 Introduction

Achieving operational resilience in today's environment is becoming more and more complex as the pace of technology and innovation continues to increase. Organizations struggle with integrating legacy and newer systems, and the outsourcing of infrastructure, software, maintenance, and security monitoring is increasing. Organizations face an increasing number of cyber attacks as well as natural, man-made, and insider incidents. An organization's ability to actively manage resilience is not only a competitive advantage but is required for long-term survival.

Sponsorship, strategic planning, and oversight of operational resilience are the most crucial activities in developing and implementing an effective operational resilience management (ORM) system. To be effective, the focus and direction of this program must come from the highest levels within the organization. It must be adequately promoted, resourced, and monitored and managed —in the same fashion as any other mission-critical program or service. Without each of these activities, an organization will not achieve and sustain sufficient operational resilience and will likely be unable to adapt and respond to its evolving risk environment.

The purpose of this technical note is to expand upon our current research on governing operational resilience. The CERT-RMM includes a process area, Enterprise Focus (EF), which describes the specific practices for sponsoring, planning, and overseeing an operational resilience management program. CERT-RMM Version 1.1 defines four maturity levels (incomplete, performed, managed, and defined). Our research highlights the need to define more granular maturity levels (which we refer to as Maturity Indicator Levels (MILs)) as a means for describing a progression of EF practices. This type of approach allows users to focus on making incremental improvements. A specific and accepted maturity scale such as the MIL sets the stage for a progression of actionable recommendations in sponsorship, strategic planning, and oversight practices.

In Section 2, we provide an overview of the CERT-RMM and the EF Process Area (PA) that serves as the foundation for our ongoing research in governing operational resilience. Section 3 provides background and an overview of seven MILs (incomplete, performed, planned, managed, measured, defined, and shared). Additional information on MILs can be found in *Advancing Cybersecurity Capability Measurement Using the CERT®-RMM Maturity Indicator Level Scale* [Butkovic 2013]. Section 4 provides a working definition of the first six MILs for each EF-specific goal. Section 5 provides a conclusion as well as a preview of additional research topics in the governance of operational resilience.

2 CERT-RMM and Enterprise Focus Overview

2.1 Overview of RMM

The CERT Resilience Management Model (RMM) is a capability maturity model for managing operational resilience. The model serves as a guide for the implementation and management of operational resilience activities. CERT-RMM is focused on the maturation of organizational capability and reflects best practices from industry and government for managing operational resilience across the disciplines of information/cyber security management, business continuity management, and aspects of IT operations management.

CERT-RMM is structured to provide organizations with a defined process for each of the 26 process areas (PAs) that support these disciplines. Each PA serves as a foundational benchmark to identify the organization's current level of capability in that specific process area. The model then provides the information needed to set desired targets for performance that are appropriate and attainable. By using an assessment based on the model, organizations are able to identify the gaps between their current state and desired targets. This information can then be used to develop action plans to close high-priority gaps.

The model's 26 PAs are organized into four categories (refer to Figure 1):

1. Enterprise Management
2. Engineering
3. Operations
4. Process Management

Figure 1: CERT-RMM 26 Process Areas by Categories

Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training and Awareness
RISK	Risk Management

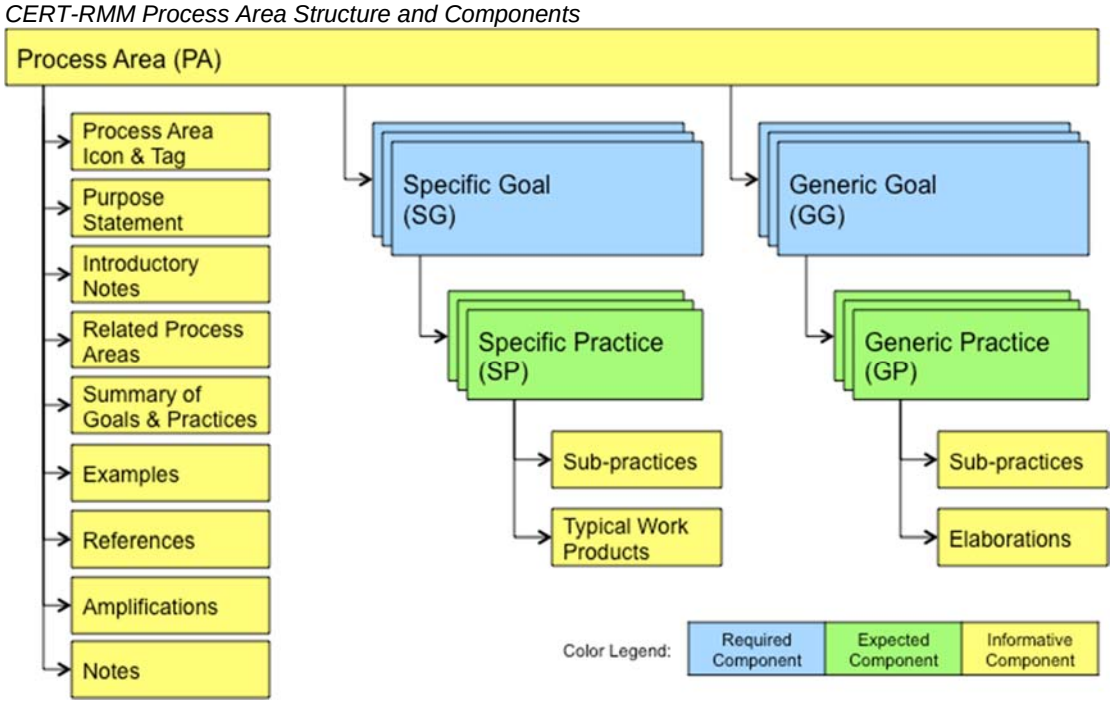
Operations	
AM	Access Management
EC	Environmental Control
EXD	External Dependencies Management
ID	Identity Management
IMC	Incident Management and Control
KIM	Knowledge and Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis and Resolution

Process Management	
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus

For each PA, the model defines required components, which describe what an organization must achieve to demonstrate capability in that PA. Within CERT-RMM, the two required components are specific goal (SG) statements and generic goal (GG) statements. Goal satisfaction, both specific and generic, is used to determine the capability level of an organization in that specific PA. The SG statements describe "what" to do to achieve the capability, whereas the GG statements describe the characteristics that must be present to institutionalize a given PA, making it part of the organization's normal course of business; part of the organization's "DNA."

The model also provides expected components, referred to as specific practices (SP) and generic practices (GP), which an organization will typically implement to achieve the required components. The SPs support goal achievement and provide a suggested way to meet the SGs. The GPs describe activities associated with ensuring the PA is effective, repeatable, and sustainable. An organization is expected to plan and achieve specific and generic practice statements (or acceptable alternatives) across each PA. Finally, for each PA, the model also includes informative components that provide guidance, suggestions, and examples to help achieve the required components. This structure is shown in Figure 2.

Figure 2: CERT-RMM Process Area Structure and Components



2.2 Overview of the Enterprise Focus Process Area

This report focuses on the EF PA within the Enterprise Management category. The purpose of the EF PA is to establish sponsorship, strategic planning, and governance over the operational resilience management (ORM) system.

Ownership and sponsorship of the ORM system by senior leaders are key components of the EF PA. Senior leaders provide the necessary level of commitment, oversight, and resources; the organization's strategic objectives are explicitly defined and aligned with the ORM system; and there are specific ORM objectives that are defined, implemented, measured, and reported across the organization. The EF SGs and SPs are shown in Table 1.

Table 1: Summary of Specific Goals (SG) and Specific Practices (SP) for the Enterprise Focus (EF) PA

EF:SG1	**Establish Strategic Objectives: *The strategic objectives are established as the foundation for the operational resilience management system.***
EF:SG1.SP1	Establish Strategic Objectives: *Strategic objectives are identified and established as the basis for resilience activities.*
EF:SG1.SP2	Establish Critical Success Factors: *The critical success factors of the organization are identified and established.*
EF:SG1.SP3	Establish Organizational Services: *The high-value services that support the accomplishment of strategic objectives are established.*
EF:SG2	**Plan for Operational Resilience: *Planning for the operational resilience system is performed.***
EF:SG2.SP1	Establish an Operational Resilience Management Plan: *A plan for managing operational resilience is established as the basis for the operational management program.*
EF:SG2.SP2	Establish an Operational Resilience Management Program: *A program is established to carry out the activities and practices of the operational resilience management plan.*
EF:SG3	**Establish Sponsorship: *Visible sponsorship of higher level managers for the operational resilience management system is established.***
EF:SG3.SP1	Commit Funding for Operational Resilience Management: *A commitment by higher level managers to fund resilience activities is established.*
EF:SG3.SP2	Promote a Resilience Aware Culture: *A resilience-aware culture is promoted through goal setting and achievement.*
EF:SG3:SP3	Sponsor Resilience Standards and Policies: *The development, implementation, enforcement, and management of resilience standards and policies are sponsored.*
EF:SG4	**Provide Resilience Oversight: *Governance over the operational resilience management system is established and performed.***
EF:SG4.SP1	Establish Resilience as a Governance Focus Area: *Governance activities are extended to the operational resilience management system and accomplishment of the process goals.*
EF:SG4.SP2	Perform Resilience Oversight: *Oversight is performed over the operational resilience management system for adherence to established procedures, policies, standards, guidelines, and regulations.*
EF:SP4.SP3	Establish Corrective Actions: *Corrective actions are identified to address performance issues.*

3 Maturity Indicator Levels (MILs)

The MILs described in this section are from *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale* [Butkovic 2013]. The purpose of developing the MIL scale specifically for CERT-RMM is to provide a scale of increased granularity for capability levels. Maturity indicator levels are a specific and more granular representation of the CERT-RMM four capability levels. The MIL scale can be highly useful when focusing on incremental improvement by providing a way to recognize shortfalls, identify incremental improvements, and measure improvement progress.

The current capability levels in CERT-RMM, as reflected in the Generic Goals, are

- Capability Level 0: Incomplete
- Capability Level 1: Performed
- Capability Level 2: Managed
- Capability Level 3: Defined

In the MIL scale, the maturity indicator levels are

- MIL0 Incomplete
- MIL1 Performed
- MIL2 Planned
- MIL3 Managed
- MIL4 Measured
- MIL5 Defined
- MIL6 Shared

For comparison purposes, the six-level MIL scale can be mapped to the existing four capability levels in CERT-RMM as shown in Table 2. This could be useful for organizations that have already begun using CERT-RMM but want to adopt the MIL scale in future improvement projects.

Table 2: Mapping of CERT-RMM Capability Levels to the MIL Scale

CERT-RMM Capability Level	MIL
Level 0: Incomplete	MIL0: Incomplete
Level 1: Performed	MIL1: Performed
Level 2: Managed	MIL2: Planned[1] MIL3: Managed MIL4: Measured[2]
Level 3: Defined	MIL5: Defined
	MIL6: Shared[3]

[1] MIL2 Planned is newly added to the original CERT-RMM capability levels.

[2] MIL4 Measured is newly added to the original CERT-RMM capability levels.

[3] MIL6 is an experimental MIL that does not map to any existing CERT-RMM capability level. It is intended to address maturity of a practice that traverses various constituencies in a community for the overall improvement of the community. For example, sharing an incident management process across many different energy com-

The definitions and attributes of each of the six MILs are as follows.

- MIL0 Incomplete indicates that a specific practice in a PA is not being performed. If MIL0 is assigned, no further assessment of maturity is performed because incomplete processes are not institutionalized.
- MIL1 Performed indicates that a specific practice in a PA is being performed. MIL1 means that there is sufficient and substantial support for the existence of the practice. Once MIL1 is attained, questions related to higher MILs can be asked to determine if the practice is institutionalized to higher degrees of maturity.
- MIL2 Planned indicates that a specific practice in a PA is not only performed but is supported by sufficient planning, stakeholders, and relevant standards and guidelines. A planned process or practice is
  - established by the organization
  - planned
  - supported by stakeholders
  - supported by relevant standards and guidelines
- MIL3 Managed indicates that a specific practice in a PA is performed, is planned, and has the basic infrastructure in place to support the process. A managed process or practice
  - is governed by the organization
  - is appropriately staffed and funded
  - is assigned to staff who are responsible and accountable for the performance of the practice
  - is performed by staff who are adequately trained to perform the practice
  - produces work products that are expected from performance of the practice and are placed under appropriate levels of configuration control
  - is managed for risk
- MIL4 Measured indicates that a specific practice in a PA is performed, planned, managed, monitored, and controlled. A measured process or practice is
  - periodically evaluated for effectiveness
  - monitored and controlled
  - objectively evaluated against its practice description and plan
  - periodically reviewed with higher level management
- MIL5 Defined indicates that a specific practice in a PA is performed, planned, managed, monitored, controlled, and consistent across all internal[4] constituencies who have a vested

---

panies that share different operating territories could improve the overall resilience of the power supply during a disruption, particularly if the process is consistent and repeatable regardless of which organization performs it.

[4] In this case, *internal* refers to constituencies over which the organization has direct managerial control.

interest in the performance of the practice. A defined process or practice ensures that the organization reaps the benefits of its consistent performance across organizational units and that all organizational units can benefit from improvements realized in any organizational unit. At MIL5, a process or practice

- is defined by the organization and tailored by individual operating units within the organization for their use
- is supported by improvement information that is collected by and shared among operating units for the overall benefit of the organization

- MIL6 Shared indicates that a specific practice in a PA is performed, planned, managed, monitored, controlled, and consistent across all internal and external[5] constituencies who have a vested interest in the performance of the practice. A shared process or practice ensures that the *community* reaps the benefits of consistent performance of the practice across many organizations bound by the community (for example, because they collectively provide a shared service such as power generation in a geographical region) and that all of the community's organizations can benefit from improvements realized in any community organization. At MIL6, a process or practice is
  - defined by the community and tailored by that community's organizations for their use
  - supported by improvement information that is collected by and shared among organizations for the overall benefit of the community

[5] In this case, *external* refers to constituencies over which the organization does not have direct managerial control.

4 MIL Scale Definitions for Enterprise-Focus-Specific Goals

In this section, we provide specific definitions for six of the seven MIL levels for each Enterprise-Focus-specific goal. MIL6 Shared is not applicable. The development and acceptance of a granular maturity scale provides a quantitative framework to identify shortfalls, identify incremental improvements, and measure improvement progress. The detailed definitions of each MIL level for Enterprise Focus specific goals are provided below.

Table 3: MIL Definitions for Specific Goal 1: Establish Strategic Objectives

MIL	SG1: Establish Strategic Objectives
MIL0: Incomplete	The organization does not use its strategic objectives as the basis for managing operational resilience. The organization may be performing some, but not all, of the following practices: establishing performance indicators and targets, critical success factors, and high-value services relevant to operational resilience.
MIL1: Performed	The organization's strategic objectives either directly or indirectly serve as the basis for managing operational resilience. There is demonstration of each of the following practices (either informally or in an ad hoc manner): establishing performance indicators and targets, critical success factors, and high-value services relevant to operational resilience.
MIL2: Planned	The organization has documented, implemented, and communicated (to all appropriate stakeholders) strategic objectives, standards, and guidelines that support managing operational resilience. The organization has documented, implemented, and communicated performance indicators and targets, critical success factors, and high-value services relevant to operational resilience. Stakeholders have accepted their roles.
MIL3: Managed	The organization has policy and oversight driving the establishment and management of strategic objectives that serve as the basis for managing operational resilience. The organization has aligned funding, staffing, and accountability to performance targets, critical success factors, and high-value services relevant to operational resilience. Risks associated with these activities are identified and managed.
MIL4: Measured	The organization periodically reviews the strategic objectives that serve as the basis for managing operational resilience, to ensure effectiveness and that the objectives are producing the intended results. Performance issues are communicated to senior management in a timely manner.
MIL5: Defined	The organization documents and shares its process(es) for establishing strategic objectives that serve as the basis for managing operational resilience across the organization. The documentation includes establishing performance indicators and targets, critical success factors, and high-value services relevant to operational resilience. Process improvements are identified, documented, and shared across the organization.

Table 4: MIL Definitions for Specific Goal 2: Plan for Operational Resilience

MIL	SG2: Plan for Operational Resilience
MIL0: Incomplete	The plan for managing operational resilience is not explicitly considered in the development of the organization's strategic plan.
MIL1: Performed	The plan for managing operational resilience is at least informally developed in conjunction with the organization's strategic planning process. The strategic planning process results in the establishment of at least an informal program for managing operational resilience in accordance with the plan.
MIL2: Planned	The strategic planning process establishes a formal plan and program for managing operational resilience. This plan is documented and communicated. Stakeholders have accepted their roles as defined in the plan.
MIL3: Managed	The organization has allocated funding, staffing, and assigned accountability to the defined plan for managing operational resilience. Risks associated with the plan are identified and managed.

MIL4: Measured	Appropriate performance data is collected, monitored, and controlled for the operational resilience management plan and program. The plan and program are periodically reviewed, evaluated, and status is reported to senior management in a timely manner.
MIL5: Defined	The organization documents and shares its process(es) for establishing and maintaining the plan and program for managing operational resilience across the organization. Process improvements are identified, documented, and shared across the organization.

Table 5: MIL Definitions for Specific Goal 3: Establish Sponsorship

MIL	SG3: Establish Sponsorship
MIL0: Incomplete	The organization has no visible sponsor for managing operational resilience.
MIL1: Performed	The organization has vis ble sponsorship by one or more executives for managing operational resilience. The organization promotes a resilience-aware culture (at least informally) through goal setting and achievement.
MIL2: Planned	The organization has established and communicated an executive sponsor for managing operational resilience. The sponsor(s) takes an active role in supporting and leading the operational resilience plan and program. The organization has a formal process for promoting a resilience-aware culture through goal setting and achievement.
MIL3: Managed	The organization's sponsor for managing operational resilience has authority and responsibility to ensure appropriate funding, staffing, accountability, training, standards, and policies. The process of promoting a resilience-aware culture through goal setting and achievement is documented and managed.
MIL4: Measured	Performance measures on the effectiveness of sponsor actions are periodically reviewed, evaluated, and reported to senior management in a timely manner.
MIL5: Defined	Not applicable; sponsor is a role, not a process.

Table 6: MIL Definitions for Specific Goal 4: Provide Resilience Oversight

MIL	SG4: Provide Resilience Oversight
MIL0: Incomplete	There is little to no oversight of the operational resilience management plan and program.
MIL1: Performed	There are (at least informal) oversight activities (establishment of charters, roles and responsibilities, processes, etc.) performed for managing operational resilience.
MIL2: Planned	There are formal oversight activities (establishment of charters, roles and responsibilities, processes, etc.) performed for managing operational resilience. Oversight activities are implemented in accordance with established policies, standards, and guidelines.
MIL3: Managed	Oversight activities for managing operational resilience are staffed, funded, and managed. Procedures are in place to manage and support oversight activities. Risks associated with oversight activities are identified and managed.
MIL4: Measured	Oversight activities for managing operational resilience are measured, monitored, and controlled to ensure the plan and program are meeting their strategic objectives. Activities are periodically reviewed and evaluated, and status is reported to senior management in a timely manner.
MIL5: Defined	The organization documents the process(es) for performing oversight activities and shares this across the organization. Process and performance improvements are identified, documented, and shared across the organization.

5 Conclusion and Next Steps

Governing operational resilience requires the appropriate level of sponsorship, a commitment to strategic planning that includes resilience objectives, and proper oversight of operational resilience activities. Organizations today are at varying levels of maturity for governing operational resilience. Recommendations for improvement are not "one size fits all." A granular, accepted, maturity scale, such as the MIL described above, allows organizations to recognize shortfalls, identify incremental improvements, and measure improvement progress. The detailed description of each MIL level for Enterprise-Focus-specific goals provides a framework for the implementation of incremental improvements in governing operational resilience.

This report is part of a series addressing the governance of operational resilience. The MIL definitions for the EF PA provide a foundation that will be used in future work to provide guidance for implementing incremental improvements in governing operational resilience.

References

URLs are valid as of the publication date of this document.

[Butkovic 2013]
Butkovic, Matthew & Caralli, Richard. *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale (CMU/SEI-2013-TN-028).* Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=69187

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	March 2015	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Defining a Maturity Scale for Governing Operational Resilience	FA8721-05-C-0003

6. AUTHOR(S)

Michelle Valdez, Julia Allen, Mary Popeck, Katie Stewart, Robert Vrtis, Lisa Young

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2015-TN-004

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Achieving operational resilience in today's environment is becoming increasingly complex as the pace of technology and innovation continues to accelerate. Sponsorship, strategic planning, and oversight of operational resilience are the most crucial activities in developing and implementing an effective operational resilience management (ORM) system. These governance activities are described in detail in the CERT® Resilience Management Model enterprise focus (EF) process area (PA). To ensure operational resilience, an organization must identify shortfalls across these defined activities, make incremental improvements, and measure improvement against a defined, accepted maturity scale. The current version of the CERT Resilience Management Model (CERT-RMM V1.2) utilizes a maturity architecture (levels and descriptions) that may not meet the granularity needs for organizations committed to making incremental improvements in governing operational resilience. To achieve a more granular approach, the CERT-RMM Maturity Indicator Level (MIL) scale was developed for application across all CERT-RMM PAs. The CERT Division of Carnegie Mellon University's Software Engineering Institute is conducting ongoing research around the current state of the practice of governing operational resilience and developing specific actionable steps for improving the governance of operational resilience. Study results provide the specific EF PA MIL scale for assessing maturity, identifying incremental improvements, and measuring improvements.

14. SUBJECT TERMS	15. NUMBER OF PAGES
operational resilience, CERT-RMM V1.2, Resilience Management Model, Maturity Indicator Level, MIL, enterprise focused	22

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL